

PATENT ABSTRACTS OF JAPAN

(11) Publication number : 09-055731
(43) Date of publication of application : 25. 02. 1997

(51) Int. Cl. H04L 9/18
G09C 1/00
G11B 20/10
// G06F 12/14

(21) Application number : 07-206351 (71) Applicant : SONY CORP
(22) Date of filing : 11. 08. 1995 (72) Inventor : SAKO YOICHIRO
OSAWA YOSHITOMO
KURIHARA AKIRA
KAWASHIMA ISAO
YONEYAMA SHIGEYUKI

(54) SIGNAL TRANSMITTING METHOD/SIGNAL RECORDING MEDIUM AND SIGNAL REPRODUCING DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent illegal use and illegal copying by preventing reproduction form information such as copy administration information and charging information to be altered or modified.

SOLUTION: A reproduction form information adding circuit 14 in a header adding circuit 13 performs data conversion for ciphering for the reproduction form information such as copy administration information and charging information from a terminal 15 according to key information from a terminal 15K and adds the converted information to data and transmits them. On a reproduction side a reproduction form information detecting circuit 25 in a header separating circuit 25 performs data conversion deciphering for the ciphered reproduction format information by using key information from a terminal 27K and the original reproduction format information is taken out of a terminal 27P.

CLAIMS

[Claim(s)]

[Claim 1]A signal transmission method performing data conversion according to key information of encryption to the above-mentioned reproduction mode information in a signal transmission method which adds and transmits reproduction mode information to an input signal.

[Claim 2]The signal transmission method according to claim 1wherein the above-mentioned reproduction mode information contains either [at least] copy management information or accounting information.

[Claim 3]The signal transmission method according to claim 1wherein the above-mentioned data conversion is performed by a logical operation of data of the above-mentioned reproduction mode informationand key information of encryption.

[Claim 4]The signal transmission method according to claim 1wherein key information of the above-mentioned encryption contains address information in part at least.

[Claim 5]The signal transmission method according to claim 1wherein the above-mentioned reproduction mode information is arranged at a position specified using position specification information.

[Claim 6]A signal transmission method arranging the above-mentioned reproduction mode information in a position specified using position specification information in a signal transmission method which adds and transmits reproduction mode information to an input signal.

[Claim 7]The signal transmission method according to claim 6wherein the above-mentioned reproduction mode information contains either [at least] copy management information or accounting information.

[Claim 8]A signal recording medium recording a signal acquired by performing data conversion according to key information of encryption to reproduction mode information added to an input signaland changing.

[Claim 9]The signal recording medium according to claim 8wherein the above-mentioned reproduction mode information contains either [at least] copy management information or accounting information.

[Claim 10]The signal recording medium according to claim 8wherein the above-mentioned reproduction mode information is arranged at a position specified using position specification information.

[Claim 11]A signal recording mediumwherein reproduction mode information added to an input signal is arranged and recorded on a position specified using position specification information and changes.

[Claim 12]A signal regeneration device which reproduces a signal recorded by performing data conversion according to key information of encryption to reproduction mode information added to an input signalcomprising:

A key information inputting means which inputs key information of the above-mentioned encryption.

A means to perform data conversion for decryption corresponding to the above-mentioned encryption according to key information from this key information inputting means.

[Claim 13]The signal regeneration device according to claim 12wherein the above-mentioned reproduction mode information contains either [at least] copy management information or accounting information.

[Claim 14]The signal regeneration device according to claim 12wherein the above-mentioned reproduction mode information is arranged at a position specified using position specification information.

[Claim 15]A signal regeneration device which is a signal regeneration device which reproduction mode information added to an input signal is arranged and recorded on a position specified using position specification informationand reproduces a signaland is characterized by having a means which takes out reproduction mode information on a position specified using the above-mentioned tab-control-specification information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to transmissionthe anti-copying of a signal and the inhibition of an unauthorized use by which record reproduction is carried out or a signal transmission method applicable to an accounting systema signal recording mediumand a signal regeneration device.

[0002]

[Description of the Prior Art]In recent yearsanti-copying and inhibition of an unauthorized use have been made important by large-scale-izing and spread of a digital recording medium of optical discs etc. Namelyin the case of digital audio information or a digital video data. Since the reproduction which does not have degradation by a copy or dubbing can be generated easily and the same data as the original data can copy easily in the case of computer datait is the actual condition which evilssuch as infringement of the copyright by an illegal copyare already producing.

[0003]Since it is sucha standard which records the information for a preventing illegal copy on an original data recording medium for the purpose of prevention of the above-mentioned illegal copy is proposedand it is used.

[0004]For exampleas a method for the above-mentioned preventing illegal copy in the digital-audio-signals recording and reproducing device called what is called R-DAT (Rotary head Digital Audio Taperecoder)To the main data area of

the digital audio signals recorded on the digital audio tape as a signal recording medium. The inhibit code (what is called SCMS: inhibit code of the standard of a serial copy management system) for forbidding prohibition and the gradual generation copy of a digital copy (namely generation restrictions) is recorded. When a digital-audio-signals recorder detects this inhibit code a method which forbids copy record of the digital audio signals concerned to a new digital audio tape top is adopted.

[0005] For example it was recorded on the signal recording medium in order to prevent the illegal copy of the Digital Video signal. It considers recording the predetermined bit ID (CGMS: inhibit code of the standard of a copy generation managerial system) for preventing illegal copy on an original digital recording medium like the method of preventing illegal copy between the recording and reproducing devices in above-mentioned R-DAT.

[0006] In the case of computer data the file content itself is enciphered using enciphering key information and carrying out using permission of it only to the registered regular user is carried out to it. This distributes the digital recording medium which information was enciphered and was recorded as a gestalt of information distribution pays a fee for the contents which the user needed obtains key information and is connected with a system which solves a code and is made available.

[0007]

[Problem(s) to be Solved by the Invention] However conventional inhibit code encryption key information etc. for signal recording media which were mentioned above are recorded on the specific place peculiar to a system accessed by the user on a recording medium as shown in JPH5-173891A.

[0008] Since it opts for the position and bit allocation on the recording medium of data reproduction mode information including copy management information accounting information etc. has a problem of unauthorized use of skipping or altering and using it. That is since reproduction mode information including copy management information accounting information etc. was in an accessible place for example from a user it was the targets of the decipherment by a malicious user or an illegal copy easily.

[0009] There is a possibility that the arrangement of compatibility of the above-mentioned reproduction mode information may be lost in each enciphering method at arbitrary places as it is fixed. If reproduction mode information is arranged fixed the technique of encryption will also be fixed it may be lacking in pliability and extendibility and a format's own life may be contracted.

[0010] This is considered as a problem not only when transmitting record reproduction transmission and reception etc. of a digital signal but when transmitting an analog signal.

[0011] This invention is made in view of the actual condition which was

mentioned aboveand is a thing.

The purpose is to provide a signal transmission methoda signal recording mediumand a signal regeneration device which make difficult an unauthorized usean illegal copyetc. by changing or altering reproduction mode informationincluding ***** etc.

[0012]

[Means for Solving the Problem]In order to solve above-mentioned SUBJECTthis invention is characterized by performing data conversion according to key information of encryption to reproduction mode information added to a signal which it is going to transmit or record.

[0013]Hereas for reproduction mode informationit is preferred for either [at least] copy management information or accounting information to be includedand to arrange this reproduction mode information in a position specified using position specification information.

[0014]This invention is characterized by arranging reproduction mode information in a position specified using position specification information.

[0015]Sinceas for enciphered reproduction mode informationthe contents are not understood without key informationit is hard to receive change and an alteration. By arranging reproduction mode informationit cannot take out in a position specified using tab-control-specification information easilyand is made it.

[0016]

[Embodiment of the Invention]It explains referring to Drawings for the desirable embodiment of this invention hereafter.

[0017]Drawing 1 is a block diagram showing roughly an example of composition of that an embodiment of the invention is applied. In this drawing 1digital data produced by carrying out digital conversion of the audio signal and video signal of an analogfor examplesuch as data and computer dataare supplied to the input terminal 11. This input digital data is sent to the sector-sized circuit 12and is sector-sized per the amount unit of prescribed datafor example2048 bytes. The sector-sized data is sent to the header additional circuit 13and the header data arranged at the head of each sector are added. These header data include reproduction mode information so that it may mention laterand this reproduction mode information has at least one side of copy management information and accounting information. The reproduction mode information on origin or an original copy is supplied to the terminal 15P of the reproduction mode information additional circuit 14and this reproduction mode information additional circuit 14According to the key information from the terminal 15Khe performs data conversion for encryption to the reproduction mode information on the agency describing aboveand is trying to add the

changed reproduction mode information. The data from the header additional circuit 13 is sent to the error correcting code-sized circuit 16data delay and a parity account are performed and parity is added in this error correcting code-sized circuit 16. In the next modulation circuit 17according to a predetermined modulation method8 bit data are changed into the modulation data of 16 channel bitsfor exampleand it sends to the synchronous additional circuit 18. In the synchronous additional circuit 18the synchronized signal of the so-called pattern of the AUTO0 velvet which breaks the modulation rule of the above-mentioned predetermined modulation method was added in predetermined data volumeand it has taken out via the output terminal 19.

[0018]The output signal from the output terminal 19 is sentfor example to a recording headand is transmitted by recording on data recording mediasuch as the shape of a disktape shapeor a semiconductoror transmitting via communication media. A playback head is reproduced from a recording mediumfor exampleor it is received via communication mediaand the transmitted signal is supplied to the input terminal 21 by the side of reproduction. The signal supplied to this input terminal 21 is the same as the signal outputted from the output terminal 19if the signal deterioration by transmissionetc. are disregarded.

[0019]The signal from the input terminal 21 is sent to the synchronization detecting circuit 22and separation of the synchronized signal added in the above-mentioned synchronous additional circuit 18 is performed. The digital signal from the synchronization detecting circuit 22 is sent to the demodulator circuit 23and processing which restores to the abnormal conditions of the above-mentioned modulation circuit 17 is performed. Specificallyit is the processing which changes 16 channel bits into 8-bit data. The digital data from the demodulator circuit 23 is sent to the error-correction-decoding circuit 24and decoding processing as inverse processing of coding in the above-mentioned error correcting code-sized circuit 16 is performed. The data by which error correction decoding was carried out is sent to the header separation circuits 25and the header of the head part of each sector is separated. The reproduction mode information in these header data is given by the data conversion of the encryption using key information as mentioned aboveand by the reproduction mode information detecting circuit 26. He performs data conversion for code decryption using the key information from the terminal 27Kand is trying to take out the decrypted reproduction mode information from the terminal 27P. It is sent to the sector decomposition circuit 28and is decomposed into the sector of the above-mentioned amount unit of prescribed dataand the remaining data in which the header was separated by the header separation circuits 25and what is called an user datum are taken out from the output terminal 29.

[0020] Heredrawing 2 shows the example of sector formatto 2048 bytes of user data area 414 bytes of synchronous field 4216 bytes of header area 43and 4 bytes of error detecting code (EDC) field 44 are addedand one sector is constituted. The error detecting code of the error detecting code field 44 comprises 32 bitsi.e. 4 bytesof CRC code generated to the user data area 41 and the header area 43. In the header area 43each field of CRC45 which is what is called a cyclic codethe playback mode information 46the layer (layer) 47 which shows which layer of a layered disk it is the address 48and the reserve 49 is provided.

[0021] The reproduction mode information 46 is 1 byte (8 bits)and has structure as shown in drawing 3for example. In this drawing 3as for 8-bit reproduction mode informationthe low rank side comprises [higher rank side] the 4-bit copy management information 52 with the 4-bit accounting information 51. As the accounting information 51the file or program containing the sector concernedThe code and flag which show whether it is no charge (freelancer)the price for viewing and listening is necessity (pay per view)or the price for copying is necessity (pay per copy) are mentioned. The 4-bit copy management information 52 is divided into the 2 more bits copy generation information 53and the copy permission / inhibition information 54 2-bit. As the 2-bit copy generation information 5300for example An original copyThe 2nd generationthe 1st generation of a copy of "01" and a copy of "10"and "11" express the copy of the 3rd [or more] generationrespectivelyand it as copy permission / inhibition information 54 2-bit00-- to two generationsa copy freelancer and "01" express the possibility of a copy10expresses the possibility of a copyand "11" expresses one generation of copy prohibitionrespectively. [for example]

[0022] When recordingfor example when transmitting dataor transmittingEncryption processing according to predetermined key information is performed without origin [it comprises the above-mentioned accounting information 51 and the copy management information 52] using original reproduction mode information as it isHe is trying to arrange this enciphered reproduction mode information to the prescribed position of the above-mentioned sector header field 43i.e. the position of the reproduction mode information 46.

[0023] Drawing 4 is a figure showing one example of performing data conversion for encryption using 8-bit key information to 8-bit reproduction mode information. That isor it is originoriginal reproduction mode information is supplied and 8-bit key information is supplied [above-mentioned] to the input terminal 61 of this drawing 4 at the input terminal 62. It is sent to the ExOR (exclusive OR) circuit 63exclusive OR is taken for every bitand these 8-bit data serves as enciphered reproduction mode information which is 8 bitsand is picked out from the output terminal 64.

[0024] Thus by performing encryption processing using key information if there is no key information the contents of the original reproduction mode information are not understood but illegal acts such as change of the contents and an alteration can be prevented effectively.

[0025] Drawing 5 shows not only key information but the example as for which a side address information for example the low rank of a sector address 8 more bit performs data conversion for encryption using 1 byte. That is in the example of this drawing 5 or it is origin original reproduction mode information is supplied 8-bit key information is supplied to the input terminal 66 and [above-mentioned] as for the low rank side of a sector address 1 byte (8 bits) is supplied to the input terminal 67 at the input terminal 65. Exclusive OR is taken for each [which is sent to the ExOR (exclusive OR) circuit 68 and corresponds] bit of every and three kinds of these 8 bit data serve as enciphered reproduction mode information which is 8 bits and are picked out from the output terminal 69.

[0026] Thus by using for the data conversion for encryption of a part of sector address the reproduction mode information enciphered for every sector changes and the preventive effect of an alteration or an unauthorized use is heightened further.

[0027] The data conversion for encryption is not limited to the example of these drawing 4 and drawing 5. For example conversion may be applied using the so-called pseudorandom numbers of an M sequence and the logical operation by AND OR EXOR NAND NOR invert circuits these combinational circuit setc. may be made to perform instead of an ExOR (exclusive OR) circuit. The transposition which changes the position of data in addition to a logical operation the substitution which replaces the value of data etc. can be used as the above-mentioned data conversion.

[0028] Next drawing 6 shows the disk shape recording media 101 such as an optical disc as an example of a recording medium. This disk shape recording medium 101 has the center hole 102 in the center. The lead-in groove (leadin) field 103 which turns into a TOC (table of contents) field which is a program management field from the inner circumference of this disk shape recording medium 101 toward a periphery. The program area 104 where program data was recorded and a program end region and what is called the lead-out (lead out) field 105 are formed. In an audio signal or the optical disc for video signal playback an audio and a video data are recorded on the above-mentioned program area 104 and this audio hour entry of a video data etc. are managed in the above-mentioned lead-in groove field 103.

[0029] Using the identification information etc. which were written in fields other than program area 104 which is data recording regions as a part of above-mentioned key information is mentioned. Specifically to the lead-in

groove field 103 which is a TOC area and the lead-out field 105. The peculiar identification information of medium manufacturing installations such as identification information for example identification information such as a serial number peculiar to a medium manufacturer identification information vendor identification information or peculiar identification information of a recorder or an encoder a cutting machine and La Stampais written in. What is necessary is just to use the above-mentioned identification information as key information for decoding a code at the time of reproduction. Identification information is written physically or chemically inside the lead-in groove field 103 this is read at the time of reproduction and it may be made to use as key information for decoding a code.

[0030] The above-mentioned reproduction mode information is recorded on arbitrary positions without fixing a recording position and writing in the tab-control-specification information for specifying the recording position of the above-mentioned reproduction mode information as a predetermined region like the TOC area of the above-mentioned lead-in groove field 103 is mentioned. In this case the recording position of the above-mentioned reproduction mode information may be directly specified for the tab-control-specification information on a TOC area and the pointer in data is specified and it may be made to specify the recording position of the above-mentioned reproduction mode information with this pointer for the tab-control-specification information on a TOC area.

[0031] That is drawing 7 shows the example which directs the recording position of reproduction mode information with the pointer 72 as tab-control-specification information in the TOC-data field 71. In this drawing 7 the pointer 71 for recording position specification of reproduction mode information comprises the sector-address information 73 the offset information 74 the number-of-bytes information 75 and attribution information. The predetermined sector 76 is specified using the sector-address information 73 on such a pointer 71. The number of bytes from offset of the reproduction mode information 77 within this sector 76 i.e. the head position of a sector to the reproduction mode information 77 is specified by the offset information 74 and the number of bytes of this reproduction mode information 77 very thing is specified using the number-of-bytes information 75.

[0032] Thus since the recording position of reproduction mode information is not fixed the situation which reproduction mode information including copy management information etc. is extracted and is changed from the same position can be effectively prevented by fixing the recording position.

[0033] As this reproduction mode information was mentioned above data conversion for the encryption using key information address etc. is performed but origin [it does not perform such data conversion] may use original reproduction

mode information.

[0034]It may be made to use a selling agency identification numbera manufacturer identification numbera recorder identification numberetc. for the sector address of a pointeroffsetetc.

[0035]Although the above is an example in the case of transmitting a digital data signalthis invention is also applicable to transmission of an analog signal.

[0036]That isdrawing 8 shows the example by which reproduction mode informationespecially copy management information were added to the analog video signal.

[0037]In this drawing 8what is called the protection code signal 81 is mixed at the predetermined horizontal period of the vertical blanking interval of an analog video signal. The horizontal period which arranges this protection code signal 81 is the 20th (H is horizontal period)H in an odd number fieldand is the 283rdH in an even number fieldfor example. This protection code signal 81 comprises the 14 bits data 82 and the 6-bit error detecting code (CRCC) 83for exampleThe 8-bit data 85 following the 6-bit header 84 in the 14-bit data 82 shows the above-mentioned reproduction mode informationespecially copy management informationand as mentioned aboveencryption processing is performed using key information.

[0038]Here as an example of the contents of the data 85 which shows 8-bit reproduction mode informationMSB(most significant bit) 86 expresses copy prohibition "1" / permission "0"The 2nd generationthe 1st generation of a copy [the following 2 bit 87 / a copy generationi.e. "00"] of an original copy and "01" and a copy of "10"and "11" express the copy of the 3rd [or more] generationrespectivelyand 4 bit 88 by the side of a low rank expresses the category code of apparatus.

[0039]By encipheringif there is no key informationin the case of such reproduction mode information on a video signalthe contents are not understoodbut change of the contents can be prevented to it.

[0040]This invention is not limited only to the example of an embodiment mentioned aboveand not only the application to the record/reproduction to a recording medium but its thing applicable to transmission of a digital signal or an analog signal generally is naturalfor example. Reproduction mode information is not limited to the above-mentioned examplebut can change various numbers of bits and contentsand it may be made to also include informationincluding the contents of saucea copied historyetc. In additionchange various in the range which does not deviate from the gist of this invention is possible.

[0041]

[Effect of the Invention]Since data conversion according to the key

information of encryption has been performed to the reproduction mode information added to the signal which it is going to transmit or record according to this invention the contents cannot be understood without key information but change and an alteration can be prevented and unjust listening an illegal copy etc. can be prevented effectively.

[0042] By arranging the enciphered reproduction mode information in the position specified using position specification information extraction of reproduction mode information can be made difficult and an unauthorized use preventive effect can be heightened further.

[0043] It also prevents arranging the reproduction mode information which is not enciphered in the position specified using position specification information from taking out reproduction mode information easily and this can prevent the unjust use by change of reproduction mode information etc.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a block diagram showing an example of the composition which can apply an embodiment of the invention.

[Drawing 2] It is a figure showing an example of sector format.

[Drawing 3] It is a figure showing an example of reproduction mode information.

[Drawing 4] It is a figure showing the example of the data conversion circuit for encryption.

[Drawing 5] It is a figure showing other examples of the data conversion circuit for encryption.

[Drawing 6] It is a figure showing an example of a data recording medium.

[Drawing 7] It is a figure showing an example which specifies the recording position of reproduction mode information with a pointer.

[Drawing 8] It is a figure for explaining the example which added reproduction mode information to the analog video signal.

[Description of Notations]

12 Sector-sized circuit

13 Header additional circuit

14 Reproduction mode information additional circuit

15K and 27K Key information input terminal

16 Error correcting code-sized circuit

17 Modulation circuit

18 Synchronous additional circuit

22 Synchronizing separator circuit

23 Demodulator circuit

- 24 Error-correction-decoding circuit
- 25 Header separation circuits
- 26 Reproduction mode information detecting circuit
- 28 Sector decomposition circuit
